PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-271309
(43)Date of publication of application : 20.09.2002

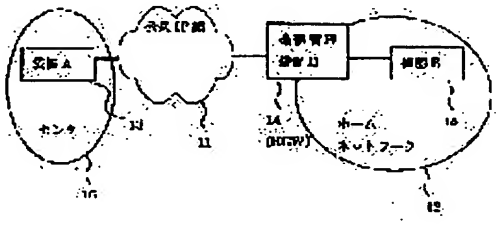
(51)Int.Cl. H04L 9/08
G06F 13/00

(21)Application number : 2001-063376
(22)Date of filing : 07.03.2001

(71)Applicant : SHARP CORP
(72)Inventor : KOBAYASHI YUTAKA

(54) KEY-INFORMATION MANAGING METHOD, AND DEVICE MANAGING EQUIPMENT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a key-information managing method and a device managing equipment wherein when a terminal outside a home network and a terminal inside the home network communicate each other, there can be eliminated the necessity of such a key exchange performed in the case of starting communication as IKE, and keys can be delivered safely to both terminals.
SOLUTION: The key-information managing method has a key AH in common between an device A 13 and an HGW 14, and has a key HB in common between the HGW 14 and the device B 15. Thus, to an access from the appliance A 13 to the device B 15, the key AH is used between the device A 13 and the HGW 14, and the key HB is used between the HBW 14 and the device B 15 as to transmit a key information AB (including a key AB) used between the devices A 13, B 15.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－271309
（Ｐ２００２－２７１３０９Ａ）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
H04L 9/08		G06F 13/00	351	Z	5B089
G06F 13/00	351		357	A	5J104
	357	H04L 9/00	601	C	

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願2001－63376(Ｐ2001－63376)

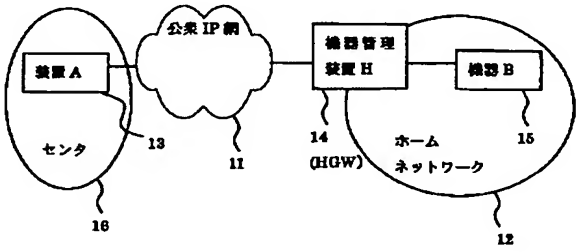
(22)出願日　平成13年３月７日(2001.3.7)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　小林　裕
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100091096
弁理士　平木　祐輔

Ｆターム(参考)　5B089 GA31 GB02 KA17 KB13 KC57 KC58 KH30
5J104 AA01 AA16 EA04 EA18 NA02 PA07

(54)【発明の名称】鍵情報管理方法及び機器管理装置

(57)【要約】
【課題】　ホームネットワーク外の端末とホームネットワーク内の端末が通信を行う際に、通信をはじめる際に行われるＩＫＥ等の鍵交換をする必要をなくすことができ、両端末に安全に鍵を配布することができる鍵情報管理方法及び機器管理装置を提供する。
【解決手段】　鍵情報管理方法は、装置Ａ１３とＨＧＷ１４との間で鍵ＡＨを共有するとともに、ＨＧＷ１４と機器Ｂ１５との間で鍵ＨＢを共有し、装置Ａ１３から機器Ｂへのアクセスに対して、装置Ａ１３とＨＧＷ１４の間は鍵ＡＨを用い、ＨＧＷ１４から機器Ｂ１５は鍵ＨＢを用いて、装置Ａ１３と機器Ｂ１５の間の鍵情報ＡＢ（鍵ＡＢを含む）を伝送する。



1

【特許請求の範囲】

【請求項１】　機器管理装置Ｈを介して外部ネットワークと接続される機器Ｂと、前記外部ネットワークに接続された装置Ａとの間の鍵情報管理方法であって、

前記装置Ａと前記機器管理装置Ｈとの間で鍵ＡＨを共有するステップと、

前記機器管理装置Ｈと前記機器Ｂとの間で鍵ＨＢを共有するステップと、

前記機器管理装置Ｈでは、

前記装置Ａから前記機器Ｂへのアクセスに対して、

前記装置Ａに対しては鍵ＡＨを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送し、

前記機器Ｂに対しては鍵ＨＢを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送ステップとを有することを特徴とする鍵情報管理方法。

【請求項２】　機器管理装置Ｈを介して外部ネットワークと接続される機器Ｂと、前記外部ネットワークに接続された装置Ａとの間の鍵情報管理方法であって、

前記装置Ａと前記機器Ｂのアクセスを許可するかを判断する判断ステップと、前記機器管理装置Ｈでは、

前記判断ステップが許可と判断したときは、前記装置Ａと前記機器Ｂとのアクセスを許可し、

前記装置Ａから前記機器Ｂへのアクセスに対して、

前記装置Ａに対しては鍵ＡＨを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送し、

前記機器Ｂに対しては鍵ＨＢを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送ステップとを有し、

前記判断ステップが否の場合には、前記伝送ステップを行わないことを特徴とする鍵情報管理方法。

【請求項３】　前記伝送ステップでは、

前記装置Ａのアドレスと前記機器Ｂのアドレスとその鍵ＡＢを含む鍵情報ＡＢを記録するステップと、

前記装置Ａと前記機器Ｂの間に前記鍵情報ＡＢが共有できている場合に、

前記装置Ａと前記機器Ｂが鍵ＡＢを用いて通信を行う際に、前記機器管理装置Ｈにおいて、前記装置Ａのアドレスと前記機器Ｂのアドレスと前記鍵情報ＡＢを一致するかチェックするチェックステップと、

前記チェックステップで一致しなかった場合に、パケットを破棄するステップとを有することを特徴とする請求項２記載の鍵情報管理方法。

【請求項４】　少なくとも１個の機器Ｂを管理下に置き、ネットワークを介して外部の装置Ａと接続された機器管理装置Ｈであって、

自己と装置Ａとの間の鍵ＡＨと、自己と機器Ｂとの間の鍵ＨＢとを記憶する記憶手段と、

前記装置Ａとの間では前記鍵ＡＨを用い、前記機器Ｂに対しては前記鍵ＨＢを用いて、前記装置Ａと前記機器Ｂとの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送手段

2

とを備えることを特徴とする機器管理装置。

【請求項５】　さらに、前記装置Ａと前記機器Ｂの間のアクセスを許可するか否かを管理するテーブルを記憶するテーブル記憶手段と、

前記管理テーブルを参照し、前記装置Ａと前記機器Ｂの通信の際に、鍵ＡＢを含む鍵情報ＡＢの伝送を制御する制御手段とを備えることを特徴とする請求項４記載の機器管理装置。

【請求項６】　通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、パケットの通過を許可／不許可するパケットフィルタリング手段と、

前記パケットフィルタリングのアクセスコントロールリスト項目に、鍵ＡＢを含む鍵情報ＡＢを記憶するパケットフィルタリング記憶手段とを備え、

前記パケットフィルタリング手段は、前記アクセスコントロールリストに基づき、パケットフィルタリングを行うことを特徴とする請求項４記載の機器管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、機器管理装置を介して外部ネットワークと接続される機器と、外部ネットワークに接続された装置との間の鍵情報管理方法及び機器管理装置に係り、特に、ネットワークにおける安全な鍵の交換が可能な鍵情報管理方法及び機器管理装置に関する。

【０００２】

【従来の技術】昨今のネットワーク・システムのオープン化・汎用化により、機密情報転送や電子商取引（Electronic Commerce）のような分野に対し、セキュリティ機能は必要不可欠なものとなっている。ネットワーク・セキュリティの目的は、ネットワークの安全保護に有り、ネットワーク・システムの機密度に応じた情報をさまざまな脅威から保護することであるとされている。一般的には、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）、否認拒否（Non-Repudiation）を維持することと定義されている。一方、ネットワークに対して想定される代表的脅威としては、盗聴、漏洩、なりすまし、改ざん／偽造、不正侵入／不正アクセス、横取り、事実の否認、破壊などである。

【０００３】また、ネットワーク・セキュリティための要素技術として、秘匿・保全技術、認証技術、鍵配送技術、否認拒否技術、第三者信用機関、アクセス管理、セキュリティ監査、セキュリティ評価基準などがある。認証とは、情報通信に関与した実体（エンティティ：人間、人間の代理として機能するプロセス、ソフトウェア、ハードウェア、通信データ等）が正当なものであるか否かを確認することであると考えられる。

【０００４】一般に、ネットワークを介して端末間で通信を行うとき、脅威としてなりすましや盗聴や改ざんと

いったものがある。これらの脅威から守るための技術に、相手や送られてきたデータが正しいかを確実に確かめる認証とパケットを盗まれても情報を見ることのできないようにする暗号化がある。認証や暗号化を行うには、鍵が必要であり、その鍵を安全に交換するしくみが鍵交換である。例えば、ＩＰｖ６（Internet Protocol version6）において実装が必須となっているＩＰｓｅｃ（Internet Protocol security）では、鍵交換でＩＫＥ（Internet Key Exchange）が規定されている。

【０００５】認証には、データを送信した相手が正しいかを確かめる通信相手認証と送られてきたデータが正しいかを確認するデータ認証がある。データ認証を行う際には、２台の端末で認証データと共通鍵を用いて、一般に一方向性ハッシュ関数を利用し相互にデータ認証を行う。通信相手認証を行うには、ＰＫＩ（Public Key Infrastructure）を利用し、署名等を用いて行う。

【０００６】暗号化を行う際には、送信側の端末において鍵を用いてデータを暗号化し送信する。受信側の端末においては、鍵を使いデータを復号化する。暗号化の場合には、共有鍵暗号方式と公開鍵暗号方式の２種類が知られている。共有鍵暗号方式では、送信側の端末と受信側の端末が同じ鍵を共有する方法であり、公開鍵暗号方式では、送信側の端末は受信側の端末の公開鍵を入手し暗号化を行い、受信側の端末は暗号化データを受け取ったら、自分しか知らない秘密鍵を用い復号化する方式である。

【０００７】認証と暗号化のどちらの場合においても、互いに持っている鍵は安全に両者がもたなければならない。従来の技術として下記（Ａ）と（Ｂ）が挙げられる。

（Ａ）一般に、ＩＰｖ６等で実装が必須となっているＩＫＥは鍵交換の従来技術としてよく知られている。ＩＫＥは、ＤＨ（Diffie-Hellman）を用いる。ＤＨは、通信を行いたい２台の端末が鍵を生成するのに必要な情報を交換し、端末側で計算を行い鍵を生成するものである。このとき、できあがる共有鍵は通信路上に流れることはなく、ＤＨを行った２台の端末にしか共有鍵はわからないという利点がある。また、鍵交換のプロトコルはファイアウォールを通過するために新たなヘッダをつけるか（処理が多くなる）、ファイアウォール側で特別に穴をあけるか（セキュリティ上問題あり）する必要があった。

【０００８】ＩＰｓｅｃでは、実際にパケットの中にＳＰＩ（Security Parameter Index）という領域を持っている。ＳＰＩを共有する端末は、セキュリティアソシエーション（ＳＡ）を持ち、ＳＰＩに対応する鍵やアルゴリズムの情報を保持する。ＳＰＩは、通常ＩＫＥの手順において決定される。実際のＳＰＩの中身は、数字のようなインデックスであって、通信路上に鍵やアルゴリズムが流れることはなく、端末がＳＰＩに対する情報（ＳＡ）を持つことになる。

【０００９】（Ｂ）また、鍵交換を行う従来技術として、管理センタを用いる方式は特開平１１－１８７０１２号公報に開示されている。管理センタを用いる方式では、まず、管理センタが、通信を行いたい２台の端末に公開鍵を配布する。管理センタの公開鍵を受けた２台の端末はそれぞれの公開鍵を管理センタに送る。管理センタは秘密値を生成し、各端末の公開鍵で暗号化して、２台の端末にそれぞれ送る。２台の端末は、それぞれ秘密値から共有鍵を計算する。この方式では、管理センタと２台の端末はそれぞれ鍵交換を行い、端末側で共有鍵の計算を行い鍵を生成する。ファイアウォールとして一般にパケットフィルタリングが知られている。これはルータ等にデフォルトで入っている機能で、従来技術では通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、決められたポリシーに基づき、パケットの通過を許可／不許可するものである。

【００１０】

【発明が解決しようとする課題】しかしながら、このような従来の共有鍵交換方法にあっては、ホームネットワークにおけるセキュリティについて、以下のような問題点があった。

（Ａ）の課題

上記したように、図１のような構成で、機器管理装置ＨＧＷを挟んだある２台の端末がセキュアな通信を始めたいとしたときにＩＫＥ等で規定されているＤＨを用いて鍵交換をする必要があった。鍵交換を行うときには認証処理があり、手間がかかる。また、間にファイアウォールを挟んだ場合に鍵交換プロトコルを通過させるのに手間がかかるなどの問題がある。

【００１１】（Ｂ）の課題

管理センタを使い鍵を配布してもらうという方法のとき、端末側でそれぞれ鍵を計算する必要があり、端末の負担が大きい。また、２台の端末の通信時に管理センタを経由するとは限らないので、端末のホームネットワークの入り口を超えられない可能性もある。

【００１２】（Ａ）と（Ｂ）共通の課題

また、２台の端末が間にファイアウォールを挟んで通信する場合に、暗号化されたデータ等を含むパケットがホームネットワーク内に入る際にパケットフィルタリングをするときに、アドレス等で現在行っているフィルタリングのレベルでしかできない。

【００１３】End-to-Endで通信する場合に、端末側でセキュリティ関連の情報を持つ場合がある。例えば、外部の認証局とやり取りするための情報であったり、通信相手端末の証明書であったりする。End-to-Endで通信する場合には、他の機関（例えば、外部の認証局）に頼らず端末側の負担を軽くしたいが、外部の認証局等の情報、通信相手端末の証明書などを持つ必要性があり、端末の負担が大きい。また、端末側では鍵を計算することも手

5

間がかかるため、この負担も大きい。

【００１４】本発明は、このような課題に鑑みてなされたものであって、ホームネットワーク外の端末とホームネットワーク内の端末が通信を行う際に、通信をはじめる際に行われるＩＫＥ等の鍵交換をする必要をなくすことができ、両端末に安全に鍵を配布することができる鍵情報管理方法及び機器管理装置を提供することを目的としている。

【００１５】

【課題を解決するための手段】本発明の鍵情報管理方法は、機器管理装置Ｈを介して外部ネットワークと接続される機器Ｂと、前記外部ネットワークに接続された装置Ａとの間の鍵情報管理方法であって、前記装置Ａと前記機器管理装置Ｈとの間で鍵ＡＨを共有するステップと、前記機器管理装置Ｈと前記機器Ｂとの間で鍵ＨＢを共有するステップと、前記機器管理装置Ｈでは、前記装置Ａから前記機器Ｂへのアクセスに対して、前記装置Ａに対しては鍵ＡＨを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送し、前記機器Ｂに対しては鍵ＨＢを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送ステップとを有することを特徴としている。

【００１６】本発明の鍵情報管理方法は、機器管理装置Ｈを介して外部ネットワークと接続される機器Ｂと、前記外部ネットワークに接続された装置Ａとの間の鍵情報管理方法であって、前記装置Ａと前記機器Ｂのアクセスを許可するかを判断する判断ステップと、前記機器管理装置Ｈでは、前記判断ステップが許可と判断したときは、前記装置Ａと前記機器Ｂとのアクセスを許可し、前記装置Ａから前記機器Ｂへのアクセスに対して、前記装置Ａに対しては鍵ＡＨを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送し、前記機器Ｂに対しては鍵ＨＢを用いて前記装置Ａと前記機器Ｂの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送ステップとを有し、前記判断ステップが否の場合には、前記伝送ステップを行わないことを特徴としている。

【００１７】また、より好ましくは、前記伝送ステップでは、前記装置Ａのアドレスと前記機器Ｂのアドレスとその鍵ＡＢを含む鍵情報ＡＢを記録するステップと、前記装置Ａと前記機器Ｂの間に前記鍵情報ＡＢが共有できている場合に、前記装置Ａと前記機器Ｂが鍵ＡＢを用いて通信を行う際に、前記機器管理装置Ｈにおいて、前記装置Ａのアドレスと前記機器Ｂのアドレスと前記鍵情報ＡＢを一致するかチェックするチェックステップと、前記チェックステップで一致しなかった場合に、パケットを破棄するステップとを有することを特徴としている。

【００１８】本発明の機器管理装置は、少なくとも１個の機器Ｂを管理下に置き、ネットワークを介して外部の装置Ａと接続された機器管理装置Ｈであって、自己と装置Ａとの間の鍵ＡＨと、自己と機器Ｂとの間の鍵ＨＢとを記憶する記憶手段と、前記装置Ａとの間では前記鍵ＡＨを用い、前記機器Ｂに対しては前記鍵ＨＢを用いて、前記装置Ａと前記機器Ｂとの間の、鍵ＡＢを含む鍵情報ＡＢを伝送する伝送手段とを備えることを特徴としている。

6

【００１９】また、より好ましくは、前記装置Ａと前記機器Ｂの間のアクセスを許可するか否かを管理するテーブルを記憶するテーブル記憶手段と、前記管理テーブルを参照し、前記装置Ａと前記機器Ｂの通信の際に、鍵ＡＢを含む鍵情報ＡＢの伝送を制御する制御手段とを備えるものであってもよい。

【００２０】また、通過するパケットの送信元アドレス、宛先アドレス、ポート番号などをチェックし、パケットの通過を許可／不許可するパケットフィルタリング手段と、前記パケットフィルタリングのアクセスコントロールリスト項目に、鍵ＡＢを含む鍵情報ＡＢを記憶するパケットフィルタリング記憶手段とを備え、前記パケットフィルタリング手段は、前記アクセスコントロールリストに基づき、パケットフィルタリングを行うものであってもよい。

【００２１】

【発明の実施の形態】以下、添付図面を参照しながら本発明の好適な鍵情報管理方法及び機器管理装置の実施の形態について詳細に説明する。

第１の実施の形態

図１は、本発明の第１の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。鍵情報管理方法として、パケット通信を行うネットワークシステムに適用した例である。

【００２２】図１において、１１は公衆Ｉ.Ｐ網、１２はホームネットワーク、１３は公衆ＩＰ網１１を介してホームネットワーク１２に接続する端末Ａ、１４はホームネットワーク１２のインタフェースとなり、プロバイダ等に接続される機器管理装置（以下、ＨＧＷ（Home Gate Way）又はＨと略記する）、１５はホームネットワーク１２内で、前記ＨＧＷ１４を用いて通信を行う端末Ｂ、１６はセンタである。

【００２３】公衆ＩＰ網１１のアクセス回線としてはＦＴＴＨ（Fiber To The Home）、ＨＦＣ（Hybrid Fiber Coax：光同軸ケーブル）、及びＡＤＳＬ（Asymmetric Digital Subscriber Line）等の大容量回線が利用可能である。ホームネットワーク１２内で、ＨＧＷ１４を用いて通信を行う機器Ｂ１５により、パケット通信を行うネットワークシステムである。ここで、装置Ａ１３はあるサービスを提供するセンタ１６の端末と考えることができる。

【００２４】図２は、上記機器管理装置Ｈ１４の詳細な構成を示すブロック図である。図２において、機器管理装置Ｈ１４は、少なくとも１個の機器Ｂを管理下に置き、ネットワークを介して外部の装置Ａ１３と接続され

た機器管理装置であり、オフラインで鍵ＡＨ及び鍵ＨＢを入力する入力手段２１と、自己と装置Ａ１３との間の鍵ＡＨを記憶する鍵ＡＨ記憶手段２２（記憶手段）と、自己と機器Ｂ１５との間の鍵ＨＢとを記憶する鍵ＨＢ記憶手段２３（記憶手段）と、鍵ＡＨ及び鍵ＨＢを基にデータ暗号化／復号化を行う暗号化／復号化手段２４と、装置Ａ１３と機器Ｂ１５の間のアクセスを許可するか否かを管理するアクセス許可／否管理テーブル２５を記憶するアクセス許可／否管理テーブル記憶手段２６（テーブル記憶手段）と、アクセス許可／否管理テーブル２５を参照し、装置Ａ１３と機器Ｂの通信の際に鍵情報ＡＢの伝送を制御するとともに、パケットフィルタリングのアクセスコントロールリスト項目に鍵情報ＡＢを加えた形で記憶するＳＡ（ＳＰＩ）制御手段２７（制御手段）と、鍵情報ＡＢを参照したアクセスコントロールリストに基づき、パケットフィルタリングを行うパケットフィルタリング手段２８と、鍵情報ＡＢで暗号化を行って外部と通信する外部通信手段２９と、鍵情報ＨＢで暗号化を行ってホーム内で通信するホーム内通信手段３０と備えて構成される。

【００２５】上記外部通信手段２９及びホーム内通信手段３０は、全体として、装置Ａ１３と機器管理装置Ｈ１４の間では鍵ＡＨを用い、また、機器管理装置Ｈ１４から機器Ｂ１５に対しては鍵ＨＢを用いて、装置Ａ１３と機器Ｂ１５との間の鍵情報ＡＢ（鍵ＡＢを含む）を伝送する伝送手段を構成している。以下、上述のように構成されたシステムの鍵情報管理方法を説明する。

【００２６】図３は、ネットワークを介した鍵情報管理方法の制御シーケンスを示す図であり、装置Ａ１３、機器Ｂ１５にＨＧＷ１４が鍵配布を行う基本的な流れを示すフローを示す。図中、ＳＴはステップ番号を示す。図３に示すように、ＨＧＷ１４を挟んだ２台の装置Ａ１３、機器Ｂ１５はそれぞれ事前にＨＧＷ１４との間にセキュアな通信路を確保しているものとする。すなわち、ステップＳＴ１において、装置Ａ１３とＨＧＷ１４は共通鍵ＡＨを持つことによりセキュアな通信路を確保し、ステップＳＴ２において、機器Ｂ１５とＨＧＷ１４は共通鍵ＨＢを持つことによりセキュアな通信路を確保している。

【００２７】このときに、ステップＳＴ３で外部にある装置Ａ１３からホーム内の機器Ｂ１５にアクセスしたいという要求をＨＧＷ１４に送る。ＨＧＷ１４は、機器Ｂ１５がホームの管理化にあるかどうかチェックを行い、機器Ｂ１５が管理化にあると判断すれば、ステップＳＴ４で機器Ｂ１５に対し装置Ａ１３のアクセスを許可するかどうかの問い合わせを送る。

【００２８】ステップＳＴ５で機器Ｂ１５はレスポンス２４を返し、機器Ｂ１５が許可すれば、ステップＳＴ６でＨＧＷ１４はそれぞれのセキュアな通信路を使って共有鍵ＡＢを装置Ａ１３と機器Ｂ１５に配布する。これ以降の、装置Ａ１３と機器Ｂ１５の通信に関しては、ステップＳＴ７で共有鍵ＡＢを用いて認証・暗号化を行い、装置Ａ１３と機器Ｂ１５の間にセキュアな通信路が確保できる。

【００２９】また、この２台の通信においては必ずＨＧＷ１４を経由する。その際、ファイアウォールのパケットフィルタリングの際にネットワークレイヤで、あて先アドレス、送信元アドレス、ポート番号等を決められたポリシーに基づいてチェック２７を行う。また、従来のアドレスやポート番号のチェックに加えて、鍵情報をチェックすることもできる（ステップＳＴ８）。

【００３０】図４は、ＨＧＷ１４がアクセス許可／否管理テーブルを管理する場合の鍵配布の流れを示す制御シーケンスを示す図である。図１の構成で図３のようなシーケンスを行うとする。このとき、実際の一例を示したものが図４である。図３と同一処理部分には同一ステップ番号を付している。図３では、装置Ａ１３から機器Ｂ１５へのアクセス要求２２がＨＧＷ１４にあった際に、ＨＧＷ１４が機器Ｂ１５に対し、アクセスを許すかどうかを直接問い合わせ（ステップＳＴ４参照）している。

【００３１】しかし、図４に示すように、装置Ａ１３が機器Ｂ１５に対するアクセスを許すかどうかをＨＧＷ１４が管理することができればこの手順は踏まなくてよく、より簡単な手順にて鍵配布が行える。ＨＧＷ１４は、どの端末がどの端末へのアクセスを許すかどうかのアクセス許可／否管理テーブル２５を持ち、これを参照することによって実現する。すなわち、ステップＳＴ１１でＨＧＷ１４はアクセス許可／否管理テーブル２５をチェックする。例えば、ステップＳＴ１２で参照されるアクセス許可／否管理テーブル２５は、装置Ａ１３から機器Ｂ１５へのアクセスはＯＫ（許可）、装置Ｃから機器Ｂ１５へのアクセスはＮＧ（不許可）となっている。

【００３２】共有鍵ＡＢに対する情報（鍵とアルゴリズム）もあわせて鍵配布の際に与えられる。この情報は、実際にはＳＰＩ、ＳＡとして与えられ、装置Ａと機器Ｂが共有鍵ＡＢを用いて通信を行う際のパケットには必ずＳＰＩがあり、そこに含まれる。このＳＰＩの情報は、ＨＧＷ１４も２台の端末と共に共有することができ、ＨＧＷ１４はパケットフィルタリングの際のポリシーを作成することができる。ＨＧＷ１４における鍵情報のチェック（ステップＳＴ１３）は、具体的にはＳＰＩのチェックとすることができる。

【００３３】次に、図２を参照して機器管理装置Ｈ（ＨＧＷ）１４の動作について詳細に説明する。

（装置Ａと機器管理装置Ｈの通信）鍵情報ＡＨは、入力手段２１を用いてあらかじめオフラインで入手することができる。入力された鍵情報ＡＨは、鍵ＡＨ記憶手段２２に格納される。外部の装置Ａから機器管理装置Ｈへの通信は、外部通信手段２９で受信される。その際の通信は、鍵ＡＨで暗号化されており、鍵情報ＡＨを読み込

み、暗号化／復号化手段２４を用いて復号を行う。

【００３４】（機器Ｂと機器管理装置Ｈの通信）鍵情報ＨＢは、入力手段２１を用いてあらかじめオフラインで入手することができる。入力された鍵情報ＨＢは、鍵ＨＢ記憶手段２３に格納される。ホーム内の機器Ｂから機器管理装置Ｈへの通信は、ホーム内通信手段３０で受信される。その際の通信は、鍵ＨＢで暗号化されており、鍵情報ＨＢを読み込み、暗号化／復号化手段２４を用いて復号を行う。

【００３５】（機器管理装置Ｈから装置Ａ及び機器Ｂへの鍵情報ＡＢの配布）図３の制御シーケンスに示すように、装置Ａから機器Ｂへのアクセス要求に対し、機器Ｂから了解を得られた場合に、鍵情報ＡＢを生成し各通信手段を用いて暗号化して通信する。また、アクセス許可／管理テーブル２５を用いることもでき、この場合には、装置Ａからのアクセス要求に対し、アクセス許可／管理テーブル２５を参照し、鍵情報ＡＢを配布するか否かの判断が入る。許可された場合には前記同様の手段で鍵情報ＡＢの配布を行う。

【００３６】（装置Ａと機器Ｂの通信）装置Ａと機器Ｂの通信は、鍵情報ＡＢを用いて暗号化される。この通信の際には、機器管理装置Ｈを必ず経由する（すなわち、外部通信手段２９とホーム内通信手段３０を通る）ので、パケットをみることができる。これがパケットフィルタリングの機能であり、その際に鍵情報ＡＢを参照し、パケットの通過の許可／不許可の決定の一役を担う。

【００３７】以上説明したように、本実施の形態の鍵情報管理方法は、装置Ａ１３とＨＧＷ１４との間で鍵ＡＨを共有するとともに、ＨＧＷ１４と機器Ｂ１５との間で鍵ＨＢを共有し、装置Ａ１３から機器Ｂへのアクセスに対して、装置Ａ１３とＨＧＷ１４の間は鍵ＡＨを用い、ＨＧＷ１４から機器Ｂ１５は鍵ＨＢを用いて、装置Ａ１３と機器Ｂ１５の間の鍵情報ＡＢ（鍵ＡＢを含む）を伝送するようにしたので、ＨＧＷ１４が外部にある装置Ａとホームネットワーク内の機器Ｂ１５に対し安全に鍵を配布することができ、装置Ａ１３から機器Ｂ１５と通信をはじめる際に行われるＩＫＥ等の鍵交換をする必要がなくなる。また、装置Ａ１３と機器Ｂ１５に安全に鍵を配布することができる。

【００３８】また、ＨＧＷ１４は、オフラインで鍵ＡＨ及び鍵ＨＢを入力する入力手段２１と、自己と装置Ａ１３との間の鍵ＡＨを記憶する鍵ＡＨ記憶手段２２と、自己と機器Ｂ１５との間の鍵ＨＢとを記憶する鍵ＨＢ記憶手段２３と、暗号化／復号化手段２４と、アクセス許可／否管理テーブル２５を記憶するアクセス許可／否管理テーブル記憶手段２６と、アクセス許可／否管理テーブル２５を参照し、装置Ａ１３と機器Ｂの通信の際に鍵情報ＡＢの伝送を制御するとともに、パケットフィルタリングのアクセスコントロールリスト項目に鍵情報ＡＢを加えた形で記憶するＳＡ（ＳＰＩ）制御手段２７と、鍵情報ＡＢを参照したアクセスコントロールリストに基づき、パケットフィルタリングを行うパケットフィルタリング手段２８と、鍵情報ＡＢで暗号化を行って外部と通信する外部通信手段２９と、鍵情報ＨＢで暗号化を行ってホーム内で通信するホーム内通信手段３０と備え、アクセス許可／否管理テーブル２５を参照し、装置Ａ１３と機器Ｂ１５の通信の際に鍵情報ＡＢの伝送を制御する。

【００３９】また、装置Ａ１３のアドレスと機器Ｂ１５のアドレスとその鍵情報ＡＢを、パケットフィルタリングのアクセスコントロールリストに追加する形で記憶し、装置Ａ１３と機器Ｂ１５の間に鍵情報ＡＢが共有できている場合には、ＨＧＷ１４において、装置Ａ１３のアドレスと機器Ｂ１５のアドレスと鍵情報ＡＢを一致するかチェックし、一致しなかった場合に、パケットフィルタリング手段２８においてパケットを破棄するように構成したので、ＨＧＷ１４通過時のパケットフィルタリングにおいても、従来行われているアドレスやポート番号に加えてＳＰＩもチェックすることができ、チェック項目が増えることになり、よりセキュアになる。

【００４０】第２の実施の形態

図５は、第２の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図であり、ホームサーバにデジタル放送ＴＶ受信機等の情報家電機器が接続されている例である。図５において、４１はインターネット、４２はホームネットワーク、４３はホームネットワーク４２内で、アドレスＤにより制御されＨＧＷ４６を用いて通信を行う複数の情報家電機器ａ．ｂ．ｃ．ｄ、４４はセンタ、４５はインターネット４１を介してホームネットワーク４２に接続するセンタ端末、４６は機器管理装置（ＨＧＷ）、４７はＬｏｏｋｕｐサーバ、４８はトップダウン・テストにおいて下位のモジュールが完成していない場合、暫定的に下位のモジュールの役目をするスタブ（Ｓｔｕｂ）である。

【００４１】ホームネットワーク４２内で、ＨＧＷ４６を用いて通信を行う情報家電機器４３により、パケット通信を行うネットワークシステムである。ホームネットワーク４２上には家庭内のあらゆる機器が接続されているとする。それらのネットワーク上のアドレスはＩＰｖ６による１２８ｂｉｔのアドレスが割り振られていて、また、それはＥＵＩ６４アドレスを含んでいる。機器の接続はイーサネット（登録商標）、ＩＥＥＥ１３９４、その他の手段でもかまわない。

【００４２】以下、上述のように構成されたシステムの鍵情報管理方法を説明する。インターネット４１に接続されたホームネットワーク４２内の複数の情報家電機器４３を、外部にあるセンタ４４の端末４５から制御・操作する例について考える。このとき、情報家電機器４３を制御するミドルウェアとしてＪiniを用いる。Ｊini

は、分散オブジェクト技術であり、オブジェクト同士が非同期の通信手順を使ってメッセージのやり取りをする機能を提供するソフトウェアなどからなる。

【００４３】Ｊiniを用いた遠隔操作の実施方法として、ホームネットワーク４２内の情報家電機器４３が、遠隔地より操作することのできるメソッドをスタブ４８としてＨＧＷ４６が持つＬｏｏｋｕｐサーバ４７に登録し、登録されたサービスについて遠隔地にあるセンタ４４の端末４５からリモートメソッドを実行し操作する。

【００４４】図６は、ホームネットワークの情報家電機器の遠隔制御の制御シーケンスを示す図である。ホームネットワーク４２内の情報家電機器４３とＨＧＷ４６は、あらかじめ、共有鍵（ＫｅｙＸ）を用いてセキュアな通信路が確保されているものとする（ステップＳＴ２０）。

【００４５】まず、ステップＳＴ２１でセンタ側の端末４５は、ホームネットワーク４２にアクセスする。ホームネットワーク４２では、情報家電機器４３を勝手に操作されてしまうと、火やガスを扱う機器などは人命に危害を及ぼしたり、ドアのロック等の防犯関係のものは施錠をはずしたりや異常通知をさせなかったり等の被害が考えられ、また、ホームバンキング等のものは財産に影響を及ぼしたりする。その他にも、家庭内の情報を見られてしまったりとか、他ネットワーク侵入の際の踏み台にされたりなど、ホームネットワーク４２の考えられる脅威はたくさんある。こういう意味では、ホームネットワーク４２というものはセキュリティがしっかりしていなければならず、ＨＧＷ４６は外部からのアクセスに対し、必ず認証を行う。これは、たとえメンテナンス等の契約をしているセンタ４４であってもきちんと認証の手順を踏まねばならない。この際の認証情報は、事前に持っているものとする。

【００４６】事前に持つ例として、センタと契約の際に認証情報をオフライン的にＨＧＷ４６がもらうことが考えられる。また、ＨＧＷ４６と情報家電機器４３側とは自己システムであるからシステム構築時に安全に鍵情報を通知することは容易である。ＨＧＷ４６は認証を行い、正しいセンタと認識できた場合に、ＯＫのレスポンスを返し（ステップＳＴ２２）、センタ側端末４５から公開鍵（ＫｅｙＡ）を受け取る（ステップＳＴ２３）。

【００４７】センタ４４は、まずホーム内の情報家電機器一覧を知る必要があり、Ｌｏｏｋｕｐサーバ４７に問い合わせを行う（ステップＳＴ２４）。ステップＳＴ２５でＬｏｏｋｕｐサーバ４７から機器の情報を得ると、リモートメソッドのスタブ４８を入手する。このスタブ４８を入手する際に、対象となる情報家電機器４３のアドレスＤや、制御したいリモートメソッドの情報がわかるステップＳＴ２６。しかし、このままではアドレスＤによりアクセスされる情報家電機器４３とはまた認証をしないと情報家電機器４３へのアクセスが許されない。

【００４８】センタ側端末４５は、ＨＧＷ４６に対し、アドレスＤによりアクセスされる情報家電機器４３へのアクセスを許可するかどうかの問い合わせを送る（ステップＳＴ２７）。ＨＧＷ４６は、その問い合わせに対し、自分の管理化にアドレスＤによりアクセスされる情報家電機器４３があり、かつセンタ側端末４５が情報家電機器４３にアクセスが許されているかどうかをチェックする（ステップＳＴ２８）。

【００４９】これがＯＫならば、センタ側端末４５に対しては公開鍵（ＫｅｙＡ）を用いて共有鍵Ｂを暗号化して送る（ステップＳＴ２９）。同様に、情報家電機器４３に対しても、事前にあるセキュアな通信路５０を用い、共有鍵（ＫｅｙＸ）を用いて共有鍵Ｂを暗号化して送る（ステップＳＴ３０）。この手順を踏むと、センタ側端末４５と情報家電機器４３が共有鍵（ＫｅｙＢ）を所有することができ、それ以降の通信（センタによる情報家電機器の遠隔操作）は安全に行うことができる（ステップＳＴ３１）。

【００５０】このように、本実施の形態によれば、ホームネットワーク内機器Ｂ側にセンタの認証情報を持つことがなくなり、ホーム内機器側の負荷が軽くなる。機器側は、鍵の計算の手間も省け、この意味でも負担が軽くなる。なお、上記各実施の形態に係る鍵情報管理方法及び機器管理装置を、上述したようなホームネットワークの情報機器管理装置に適用することもできるが、勿論これには限定されず、暗号通信システムであれば全ての装置に適用可能である。また、上記鍵情報管理装置を構成する各手段の種類、数及び接続方法などは前述した各実施の形態に限られない。

【００５１】

【発明の効果】以上、詳述したように、本発明によれば、機器管理装置が外部にある装置Ａとホームネットワーク内の機器Ｂに対し安全に鍵を配布することができるので、装置Ａから機器Ｂと通信をはじめる際に行われるＩＫＥ等の鍵交換をする必要がなく、装置Ａと機器Ｂに安全に鍵を配布することができる。

【００５２】機器管理装置通過時のパケットフィルタリングにおいても、従来行われているアドレスやポート番号に加えてＳＰＩもチェックすることができ、チェック項目が増えることになり、よりセキュアになる。また、ホームネットワーク内機器Ｂ側にセンタの認証情報を持つことがなくなり、ホーム内機器側の負荷を軽くすることができる。また、機器側は、鍵の計算の手間を省くことができ、機器側においても負担を軽くすることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。

【図２】本実施の形態の鍵情報管理方法が適用されるネットワークの機器管理装置の詳細な構成を示すブロック

図である。

【図３】本実施の形態のネットワークを介した鍵情報管理方法の制御シーケンスを示す図である。

【図４】本実施の形態の機器管理装置がアクセス許可／否管理テーブルを管理する場合の鍵配布の流れを示す制御シーケンスを示す図である。

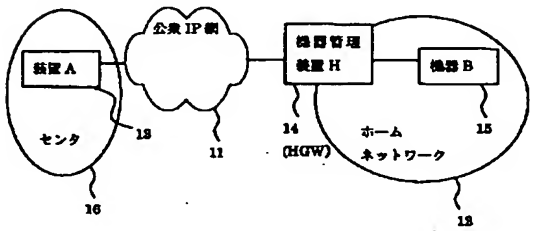
【図５】第２の実施の形態の鍵情報管理方法が適用されるシステムの構成を示す図である。

【図６】本実施の形態のホームネットワークの情報家電機器の遠隔制御の制御シーケンスを示す図である。

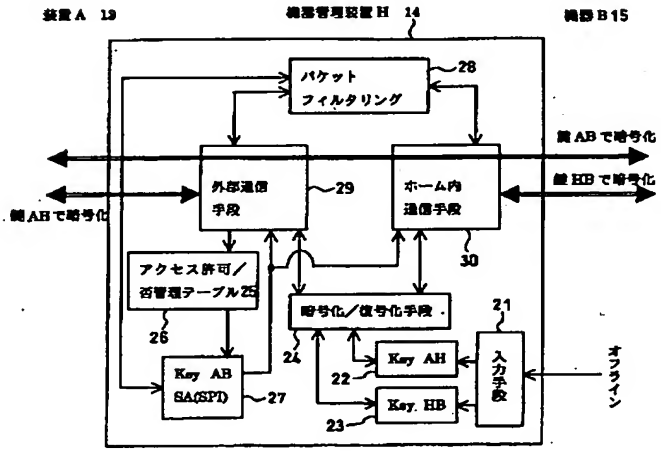
【符号の説明】

１１　公衆ＩＰ網
１２，４２　ホームネットワーク
１３　端末Ａ
１４，４６　機器管理装置（ＨＧＷ，Ｈ）
１５　端末
１６，４４　センタ
２１　入力手段
２２　鍵ＡＨ記憶手段（記憶手段）
２３　鍵ＨＢ記憶手段（記憶手段）
２４　暗号化／復号化手段
２５　アクセス許可／否管理テーブル
２６　アクセス許可／否管理テーブル記憶手段（テーブル記憶手段）
２７　ＳＡ（ＳＰＩ）制御手段（制御手段）
２８　パケットフィルタリング手段
２９　外部通信手段
３０　ホーム内通信手段
４１　インターネット
４３　情報家電機器
４５　センタ端末
４７　Ｌｏｏｋｕｐサーバ
４８　スタブ（Ｓｔｕｂ）

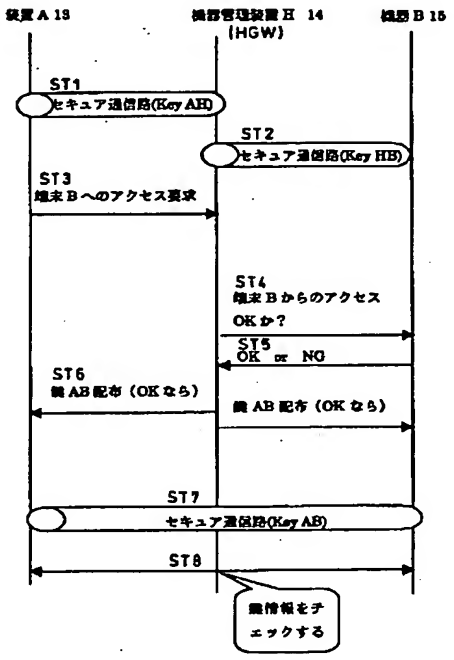
【図１】



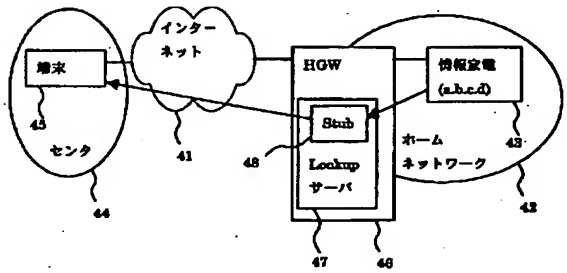
【図２】



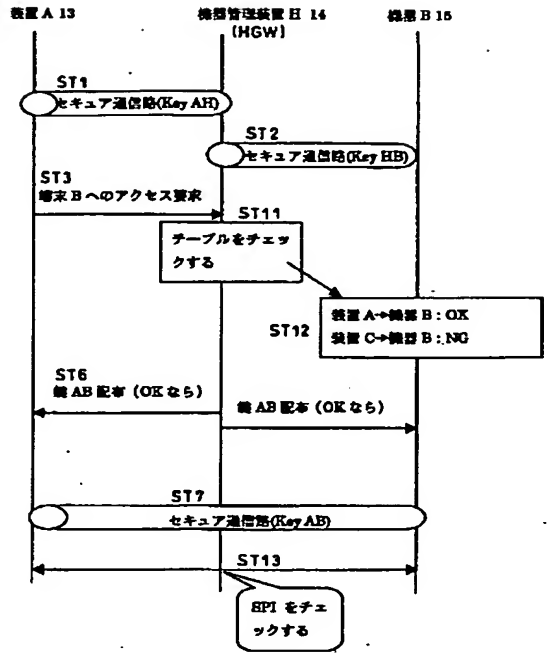
【図３】



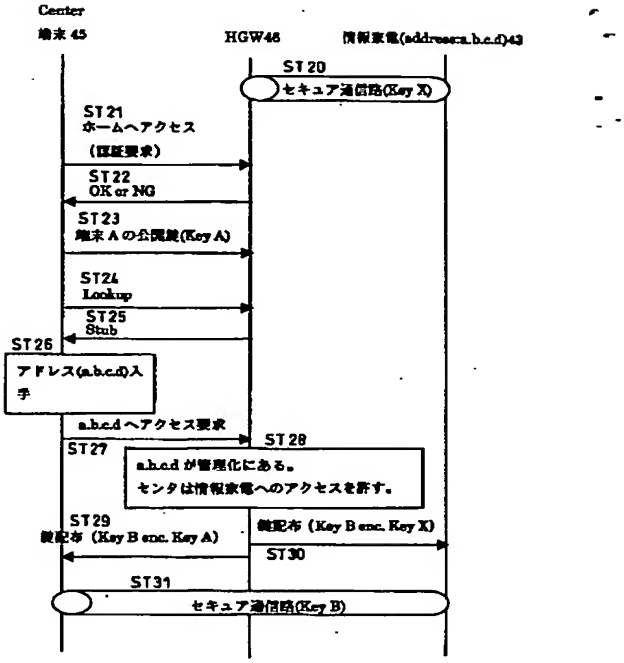
【図５】



【図４】


装置 A 13
機器管理装置 H 14
(HGW)
機器 B 15
ST1
セキュア通信路(Key AH)
ST2
セキュア通信路(Key HB)
ST3
端末 B へのアクセス要求
ST11
テーブルをチェックする
ST12
装置 A→機器 B : OK
装置 C→機器 B : NG
ST6
鍵 AB 配布 (OK なら)
鍵 AB 配布 (OK なら)
ST7
セキュア通信路(Key AB)
ST13
SPI をチェックする

【図６】


Center
端末 45
HGW46
情報家電(address a.b.c.d)43
ST20
セキュア通信路(Key X)
ST21
ホームへアクセス
(認証要求)
ST22
OK or NG
ST23
端末 A の公開鍵(Key A)
ST24
Lookup
ST25
Stub
ST26
アドレス(a.b.c.d)入手
a.b.c.d へアクセス要求
ST27
ST28
a.b.c.d が管理化にある。
センタは情報家電へのアクセスを許す。
ST29
鍵配布 (Key B enc. Key A)
鍵配布 (Key B enc. Key X)
ST30
ST31
セキュア通信路(Key B)